

1804.203

Work, to the NASA Center for Aero-Space Information (CASI), Attention: Document Processing Section, 7121 Standard Drive, Hanover, MD 21076-1320.

[64 FR 36606, July 7, 1999]

1804.203 Taxpayer identification information.

Instead of using the last page of the contract to provide the information listed in FAR 4.203, NASA installations may allow contracting officers to use a different distribution method, such as annotating the cover page of the payment office copy of the contract.

[64 FR 1528, Jan. 11, 1999]

Subpart 1804.4—Safeguarding Classified Information Within Industry

1804.402 General.

(b) NASA security policies and procedures are prescribed in NPD 1600.2A, NASA Security Policy; NPG 1600.6A, Communications Security Procedures and Guidelines; NPG 1620.1, Security Procedures and Guidelines; NPG 2810.1 and NPD 2810.1 Security of Information Technology.

[66 FR 53546, Oct. 23, 2001]

1804.404-70 Contract clause.

The contracting officer shall insert the clause at 1852.204-75, Security Classification Requirements, in solicitations and contracts if work is to be performed will require security clearances. This clause may be modified to add instructions for obtaining security clearances and access to security areas that are applicable to the particular acquisition and installation.

1804.470 Security requirements for unclassified information technology resources.

1804.470-1 Scope.

This section implements NASA's acquisition-related aspects of Federal policies for assuring the security of unclassified automated information resources. Federal policies include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*), the Clinger-Cohen Act of 1996 (40 U.S.C.

48 CFR Ch. 18 (10-1-02 Edition)

1401 *et seq.*), Public Law 106-398, section 1061, Government Information Security Reform, OMB Circular A-130, Management of Federal Information Resources, and the National Institute of Standards and Technology security guidance and standards.

[67 FR 48815, July 26, 2002]

1804.470-2 Policy.

(a) NASA policies and procedures on security for automated information technology are prescribed in NPD 2810.1, Security of Information Technology, and in NPG 2810.1, Security of Information Technology. The provision of information technology (IT) security in accordance with these policies and procedures, is required in all contracts that include IT resources or services in which a contractor must have physical or electronic access to NASA's sensitive information contained in unclassified systems that directly support the mission of the Agency. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include:

(1) Computer control of spacecraft, satellites, or aircraft or their payloads;

(2) Acquisition, transmission or analysis of data owned by NASA with significant replacement costs should the contractor's copy be corrupted; and

(3) Access to NASA networks or computers at a level beyond that granted the general public, e.g. bypassing a firewall.

(b) The contractor must not use or redistribute any NASA information processed, stored, or transmitted by the contractor except as specified in the contract.

[66 FR 36491, July 12, 2001]

1804.470-3 Security plan for unclassified Federal Information Technology systems.

(a) The requiring activity with the concurrence of the Center Chief Information Officer (CIO), and the Center Information Technology (IT) Security Manager, must determine whether an